Ricardo A. Vittoni - FSS

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

SISTEMAS DE SEGURIDAD PARA QUEMADORES (BMSIS)

SAFETY NOTE SN - 5032

IMPLEMENTACIÓN DE NIVEL SIL 3 A NIVEL FUNCIONAL Y DEL HARDWARE

1. El Nivel SIL no está "dentro del Logic Solver"

Continuando con el análisis sobre la Evaluación e Implementación del Nivel SIL para Quemadores (ver Nota de Seguridad SN-5031), veo la necesidad de aclarar un concepto erróneo que suele esgrimirse durante el diseño de un BMSIS: la creencia equivocada de que bastará con proveer un "PLC SIL 3" (como suele decirse), para que el BMSIS provea el nivel de protección adecuado. Este concepto equivocado presupone que el Nivel SIL está "dentro del Logic Solver" y que éste, en forma "mágica" se encargará de resolver nuestro problema de seguridad.

Digamos una vez más, que **el Nivel SIL es sólo una de las características de la Función Instrumentada de Seguridad** (SIF), y que ésta es en realidad **como una "cadena" en la cual todos sus eslabones deben proveer "la misma resistencia para evitar que ella se rompa"**.

Es decir, **es la SIF completa la que provee un determinado Nivel de Reducción de Riesgo, el cual está relacionado con el Nivel de Integridad SIL** (o grado de "certeza" con el cual será ejecutada esta acción protectora), **y con el Tiempo de Seguridad** (el cual no deberá ser excedido si se quiere evitar el accidente).

Cada SIF es en sí misma una "cadena de seguridad" que está compuesta por "eslabones físicos" (hardware) y por "eslabones funcionales" (software y/o firmware).

En particular, la parte física de la "SIF de shutoff por apagado de llama" está formada por:

H1) Sistemas de Detección de Presencia de Llama

H2) Sistemas de Corte de Combustible

H3) Hardware del Logic Solver (canales de Entrada/Salida y CPU)

H4) Cableado entre los componentes (detectores - logic solver - actuadores)

Por otro lado, la parte funcional de la "SIF de shutoff por apagado de llama" está compuesta por:

F1) Características Funcionales de los Detectores de Llama (Discriminación, Autodiagnóstico, Tiempo de Reacción, Funcionamiento FailSafe)

F2) Características Funcionales de los Sistemas de Corte de Combustible (Forma de Bloqueo, Tiempo de Reacción, Capacidad de Diagnóstico, Funcionamiento FailSafe)

F3) Características Funcionales del Logic Solver (Lógica Parametrizable o Programable, Protección de Acceso, Forzado de entradas/salidas, Autodiagnóstico, Tiempo de Ejecución, Diagnóstico de la Instalación, Diagnóstico de Dispositivos de Campo, Funcionamiento FailSafe)

No analizaremos cada una de estas características en forma individual, ya que muchas de ellas han sido cubiertas en otras Notas de Seguridad anteriores, sino que nos limitaremos a elaborar una guía práctica adecuada para la implementación de esta SIF de Shutoff por apagado de llama, de forma tal de obtener el Nivel SIL 3 "a lo largo" de TODA la "cadena de seguridad".

2. Uniendo los Conceptos de Seguridad Funcional y Tolerancia a Fallas

Aunque tanto la Norma IEC 61508 como su derivada para la Industria de Procesos, IEC 61511, mencionan la necesidad de proveer Tolerancia a Fallas, tanto en los dispositivos de campo (Detectores y Actuadores), como en el Logic Solver, ninguna de ellas explícita qué significa realmente esta "tolerancia".

En términos generales, en estas Normas se entiende por "tolerancia a fallas" la capacidad de un sistema de "seguir funcionando, aún en presencia de una falla, sin dejar de ejercer su función protectora", como en el caso de los Logic Solvers tipo TMR o 1oo2D, por citar dos ejemplos.

Pero ¿hasta cuándo un sistema podrá seguir funcionando en presencia de esta falla sin perder su capacidad protectora?

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

Para poder contestar esta pregunta será necesario incorporar los conceptos establecidos por la Norma IEC 62061 (Seguridad Funcional en Máquinas), la cual incluye las prescripciones de la Norma ISO 13849.
La Norma ISO 13849 (internacionalización de la Norma Europea EN 954), establece cinco Categorías de Seguridad, de cuya definición se comprende claramente el significado de la frase "tolerancia a fallas". Analizaremos solamente la definición de la Categoría 4, pues es la que nos permitirá implementar el Nivel SIL 3 que necesitamos.

En Categoría 4, la Tolerancia a Fallas debe aplicarse de forma tal que a) **"una sola falla en cualquiera de sus partes no cause la pérdida de la función de seguridad"**, b) **"la primera falla se detecte ante la siguiente demanda de la función de seguridad, o antes de ésta"**, c) **"si esta detección no es posible, entonces una acumulación de fallas no causará una pérdida de la función de seguridad"**.

Como puede verse claramente, la definición de la Categoría 4 explica la "tolerancia a la primer falla", es decir, la falla de un componente primario debe ser detectada por algún otro componente secundario, en forma inmediata o al presentarse una demanda del sistema de protección.

Pongamos como ejemplo el corte de energía que deberá aplicarse al solenoide de comando de una válvula de shutoff de combustible, con Tolerancia a Fallas = 1.
Para garantizar este corte, se dispondrán dos contactores que cortarán la alimentación a cada uno de los extremos del solenoide (ver también el punto 3.2).
Si, por ejemplo, uno de los contactores quedara "pegado" luego de una parada de emergencia, el sistema continuaría siendo seguro pues el segundo contactor tendría aún la capacidad de cortar la alimentación del otro extremo de la bobina. Esta es la "Tolerancia a Fallas = 1" requerida.

La pregunta que cabe hacerse es ¿al detectar la falla del primer contactor, el sistema deberá permitir un re-arranque "sabiendo" que le queda un solo contactor para cortar la alimentación?
Si el sistema es Categoría 4, **la respuesta es NO**, porque, tal como dice la definición, "una acumulación de fallas no causará una pérdida de la función de seguridad", lo cual sucedería si fallara el segundo contactor sin que se hubiera reparado el primero.

Pero hasta aquí la Norma ISO nos da una respuesta a medias, es decir, nos habla de la tolerancia a fallas, pero no del Nivel SIL, pues en ella no se consideran las "probabilidades de falla en demanda". Sin embargo, establece una relación entre las Categorías y el Nivel SIL, que puede explicarse así para el Nivel SIL que nos interesa:

- **Para obtener un Nivel SIL 3, los componentes de la "cadena de seguridad" deberán estar conectados de acuerdo con la Categoría 4**.

Y esto es así porque, como podrá comprenderse, los componentes eléctricos y/o electrónicos presentan "modos de falla complejos", es decir, que pueden fallar en diferentes formas y generar así situaciones de peligro (ver punto 4.1.2).

Cabe aclarar sin embargo, que un subsistema de Categoría 4 no necesariamente provee un Nivel SIL 3, aunque un subsistema de Nivel SIL 3, necesariamente deberá estar cableado según Categoría 4.

Pero, ¿cómo implementar esto "físicamente"? Veamos algunos ejemplos tomados de sistemas existentes en el mercado.

3. Parte física de la "SIF de shutoff por apagado de llama"

3.1 Conexión de señales de Entrada al Logic Solver

Sobre la base de lo explicado en el punto 2, **los Sistemas de Detección de Llama** (sean éstos del tipo "Flame Rod" u "Ópticos por Radiaciones UV y/o IR"), **DEBEN proveer al menos dos contactos independientes para la "señal de apagado de llama"**, de forma tal que el sistema pueda detectar la "primera falla".

Ambos contactos deberán ser llevados a canales independientes del Logic Solver, tal como muestra la Figura 3.1.1, en la cual puede verse cómo (por medio de la alimentación independiente por trenes de pulsos de diferente frecuencia para cada contacto), el Logic Solver podrá detectar dicha primera

falla (cable cortado, cable a masa, etc.), **enviando el sistema a condición segura ANTES que se produzca una segunda falla** (ISO 13849 Categoría 4).

Sin perjuicio de esto, **deberán utilizarse dos Sistemas de Detección de llama** (el gráfico muestra la conexión de uno sólo de ellos) **para garantizar la detección de la primera falla a nivel "funcional"** (ver punto 4).

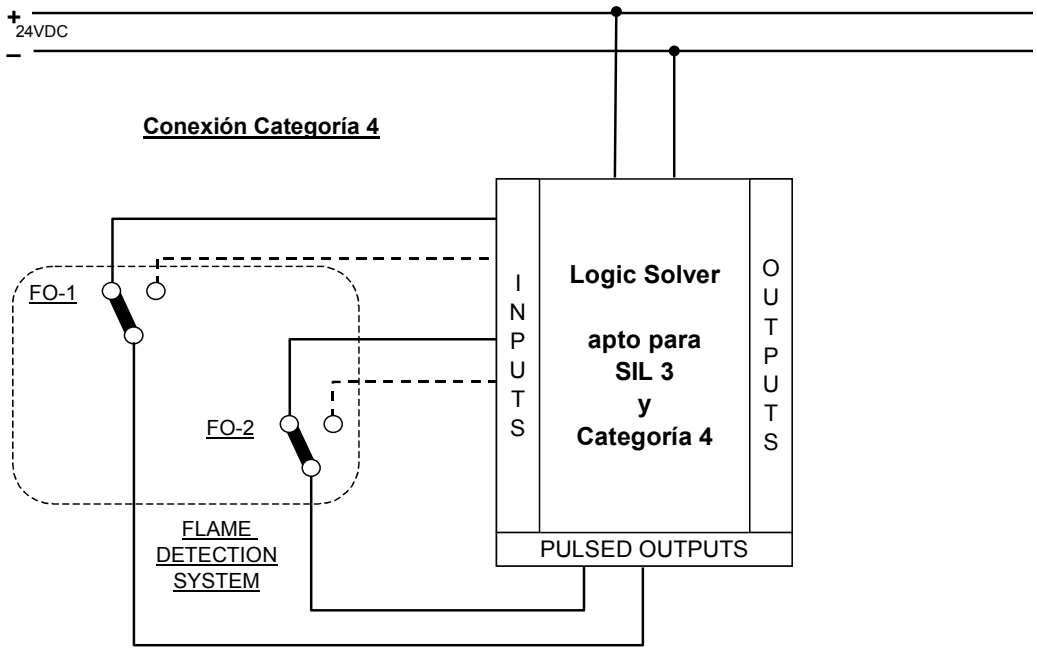


Fig. 3.1.1

3.2 Conexión de señales de salida del Logic Solver

El tipo de Sistema de Corte de Combustible a proveer dependerá del tipo de combustible que estemos utilizando pero, en lo que se refiere a la Tolerancia a Fallas, ésta será igual a 1 a fin de garantizar el bloqueo del mismo, como analizáramos en el punto 2.

Como hemos analizado en otras Notas de Seguridad, el Nivel SIL que se requiere para esta SIF puede garantizarse con válvulas de shutoff independientes o con Sistemas de Bloqueo y Venteo que proveen un único comando de actuación (Válvulas de Triple Efecto o "Trifecta").

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

La Figura 3.2.1 nos muestra una forma de conexión que permite la desenergización segura del Sistema Trifecta (hemos indicado este esquema por simplicidad; para la desconexión de válvulas de shutoff y bloqueo independientes, deberán triplicarse las entradas/salidas).

Tal como analizáramos en el punto 2, esta conexión permite detectar una eventual primera falla de uno de los contactores de salida y **enviar al corte al segundo contactor antes de que una segunda falla pueda hacer perder la seguridad**.

Asimismo, cuándo uno de estos contactores no haya accionado adecuadamente, **se evitará una nueva energización del Sistema Trifecta hasta que no haya sido corregida la falla** (ISO 13849 Categoría 4).

Cabe hacer notar que, para que esta protección sea efectiva, C1 y C2 **deben** ser contactores de seguridad con contactos "positivamente guiados", según IEC 60947.

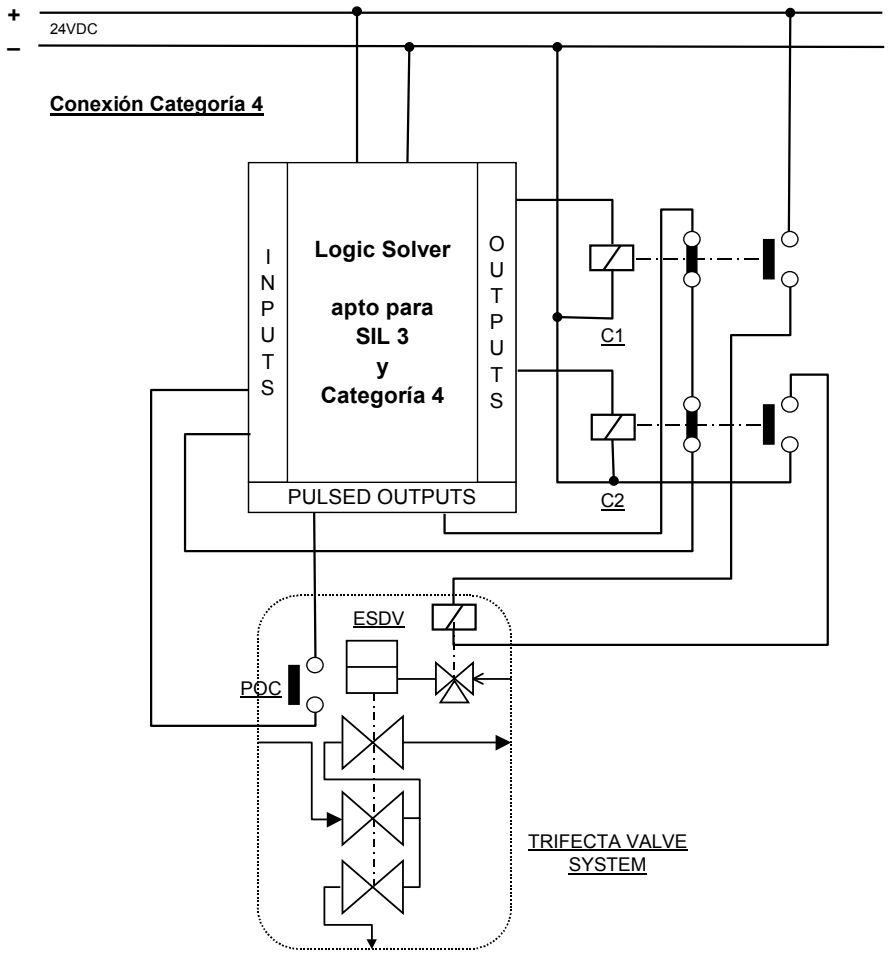


Fig. 3.2.1

4. Parte Funcional de la SIF de shutoff por apagado de llama

4.1 Características Funcionales de los Sistemas de Detección de Presencia de Llama

Actualmente los principales Sistemas de Detección de Presencia de Llama más usados son los del tipo "Flame Rod" y los del tipo "Óptico por Radiaciones UV y/o IR".

En los Sistemas con Flame Rod, la presencia de la llama se detecta por el nivel de la componente de corriente contínua que fluye desde la varilla de detección (Flame Rod) a masa, a través de la llama.
Estos Sistemas son utilizados desde hace mucho tiempo y la única "ventaja" que quizá posean es su simplicidad, aunque su funcionamiento se ve afectado en quemadores que funcionan con combustible líquido (Fuel Oil), debido a los depósitos de carbón que se producen en la Varilla durante el funcionamiento, lo cual obliga a una limpieza periódica y permanente de la misma.

Los Sistemas que detectan la Radiación de la llama, en cambio, por ser más sofisticados y por no estar en contacto directo con la llama, proveen un funcionamiento que no es afectado por el tipo de combustible.
Estos Sistemas (de los cuales hemos hablado ampliamente en la SN-011), permiten además "analizar" la llama por medio de sus radiaciones (tanto UV como IR).

Pero independientemente del tipo de Detector de Presencia de Llama que utilicemos y como explicamos en la SN-5031, a fin de preservar la Seguridad Funcional del "lazo de seguridad", **se necesitarán al menos dos Sistemas de Detección de Llama en votación para garantizar el adecuado nivel de tolerancia a fallas en una SIF de Nivel SIL 3** (además, cada uno de estos Sistemas de Detección deberá ser conectado al Logic Solver según los lineamientos establecidos en el punto 3.1.).

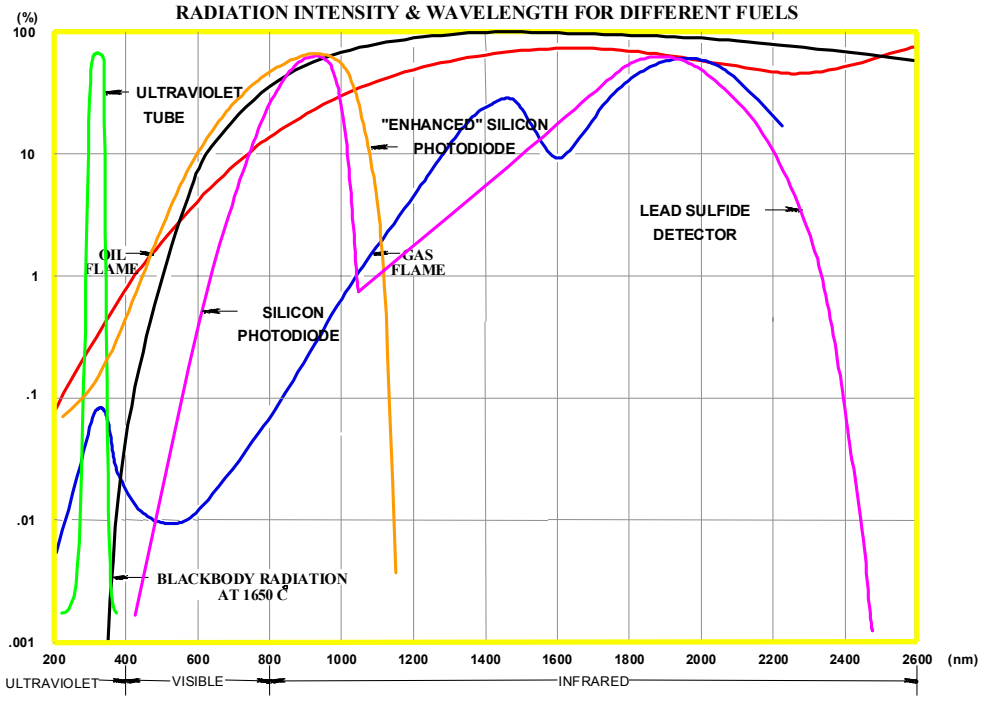
4.1.1 Discriminación

Una de las características funcionales fundamentales para garantizar un adecuado nivel de protección del BMSIS, es la capacidad de discriminación del Detector de Presencia de Llama. Esta

capacidad permitirá al Sistema de Detección saber si la llama que está "detectando" es la correspondiente a un apropiado funcionamiento del Quemador o si, por el contrario, se trata de una "falsa llama" que pondrá en peligro la seguridad de la Caldera o del Horno.

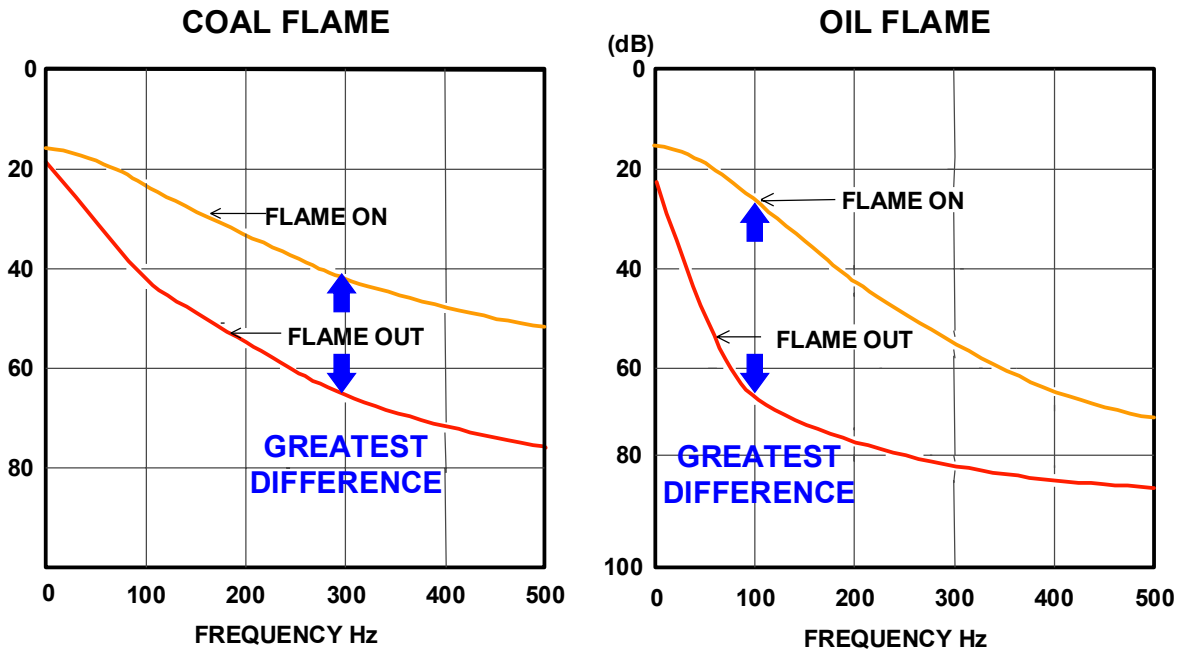
Los Sistemas del tipo "Flame Rod" no poseen discriminación, en la medida en que **miden solamente la corriente que pasa por la varilla en ese momento a través de la supuesta llama, pero no pueden determinar si la llama es apropiada**, lo cual sí pueden discernir los Sistemas del tipo Óptico (radiaciones UV y/o IR).
De todas formas, **un buen Sistema Flame Rod podrá detectar una varilla "sucia" y enviar el BMSIS a condición segura cuando considere que la detección puede ser no eficaz o insegura**.

Los Sistemas del tipo Óptico permiten un alto grado de discriminación en la medida en que "ven" la llama (y no sólo detectan su presencia como en el caso del Flame Rod).
Es muy importante hacer notar, sin embargo, que **cada tipo de combustible provee un espectro de radiación distinto** (como vemos en el siguiente gráfico), **y que es precisamente el Sistema de Detección de Presencia de Llama el encargado de analizarlo utilizando detectores del tipo UV, IR, o una combinación de ambos** (en el gráfico se indica, además, la sensibilidad para cada tipo de detector):



Como puede observarse en el gráfico (gentileza de IRIS Systems Inc.), la radiación propia del hogar podría ser detectada como llama si los detectores tipo IR solamente observaran el espectro de frecuencia de la radiación.

Para evitar esto, los Sistemas de Detección IR analizan el "parpadeo" de la llama (flickering), que se produce al mezclar el combustible con el aire de combustión, utilizando filtros de frecuencia ajustables que permiten que el detector IR provea tan buena discriminación como la que ofrecen los Sistemas UV en su angosto rango de frecuencias (en el siguiente gráfico se muestran dos ejemplos donde se ve cómo cambia la frecuencia de lectura del detector IR para combustibles distintos; la curva roja muestra la "radiación de fondo" del hogar, la cual confundiría al detector si éste no utilizara los filtros adecuados).



Pero sin lugar a dudas, **la mejor solución, que garantiza una perfecta discriminación al mismo tiempo que provee una tolerancia a fallas en el mismo detector, la constituyen los Sistemas de Detección de Llama Duales UV+IR**.

En éstos, prácticamente el único elemento en común es la lente en el frente del Detector, toda vez que, **tanto los sensores UV e IR, como sus circuitos electrónicos asociados y las señales de**

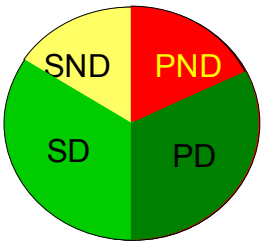
salida de presencia de llama duplicadas, son totalmente independientes desde el punto de vista funcional, garantizando una tolerancia a fallas = 1 inherente al Sistema (no obstante se recomienda, siempre que sea posible, sobre todo en Quemadores de gran porte, la utilización de dos Sistemas por Quemador).

Estos Sistemas suelen incorporar, además, **un relé de falla independiente para cada canal** (uno para el UV y otro para el IR).

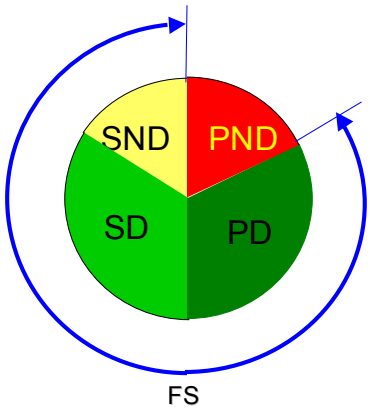
4.1.2 Autodiagnóstico FailSafe

La capacidad de autodiagnóstico, a la cual aludiéramos en otras Notas de Seguridad, es la que permite a un sistema "saber" cuándo algo no está funcionando bien en su seno.

Esta capacidad de detectar fallas propias permite clasificar a estas últimas en 4 categorías, como muestra el gráfico:



- Failure Rate Global
  - Fallas Seguras
    - **SD = Segura Detectada**
    - **SND = Segura NO Detectada**
  - Fallas Peligrosas
    - **PD = Peligrosa Detectada**
    - **PND = Peligrosa NO Detectada**



Cuando la falla sea “segura” o se detecte una falla peligrosa, el subsistema irá a condición segura, es decir, a una condición en la cual se garantice que la protección provista por el mismo continuará siendo efectiva, aún en presencia de dicha falla.

A este comportamiento se lo conoce como **FAILSAFE** (FS)

Cuando el autodiagnóstico detecta una falla y envía al subsistema a condición segura, es decir, a una condición en la cual se garantiza que la protección provista por el mismo continuará siendo efectiva, aún en presencia de dicha falla, se lo conoce como **Autodiagnóstico FailSafe**.

Pero cabe preguntarse, ¿qué pasará con las fallas que el autodiagnóstico no puede descubrir?

4.1.3 Tasa de Fallas Peligrosas (FRD - Failure Rate Dangerous)

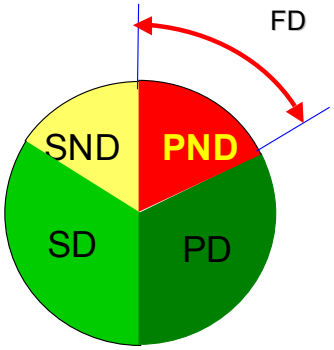
Como vemos en la figura, existe un porcentaje de las posibles fallas que no podrán ser detectadas por el autodiagnóstico failsafe, el cual reacciona sólo ante las fallas del tipo SD y DD.
Este porcentaje no cubierto por el autodiagnóstico es muy bajo en equipos de alta calidad y su valor se mide en fallas por año o en millonésimos de fallas por hora.

Por ejemplo, un buen Sistema de Detección de Presencia de Llama tendrá un FRD menor que una falla peligrosa cada 5000 años, la cual podrá expresarse como:

FRD = 1 / 5000 años ó FRD = 2,28E-8 / hora

Si recordamos los valores que exige la IEC 61508 para el modo contínuo de operación, veremos que este valor se halla dentro de los límites del Nivel SIL 3.

Sin embargo, **no debe olvidarse que la utilización de dos Sistemas de Detección de Presencia de Llama es obligatoria** para asegurar los niveles de tolerancia a fallas requeridos para este Nivel SIL (ver punto 2).



Cuando los circuitos de autodiagnóstico no puedan detectar una falla no podrán enviar al subsistema a condición segura (FAILSAFE).

En estas circuntancias, si la falla es peligrosa, el comportamiento será

Fail-to-Danger o

FAIL ON DEMAND (FD)

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

4.1.4 Tiempo de respuesta ante la falta de llama (FFRT)

Como ya hemos analizado en notas anteriores, existe un tiempo máximo de respuesta para toda SIF. Este tiempo es necesariamente menor que el tiempo mínimo que pudiera convertir el proceso en un evento peligroso (tiempo conocido como Process Safety Time o PST).

Como vimos en la SN-5031, el tiempo máximo establecido por la Norma FM 7605 para producir el shutoff de combustible una vez detectada la falta de llama, es de tan sólo 4 segundos.

Si consideramos que un buen Sistema de Corte de Combustible no tardará más de 1 segundo en cerrar, una vez recibida la señal desde el Logic Solver, y descontando el tiempo de procesamiento de este último, usualmente del orden de sólo algunos milisegundos, **el tiempo máximo que podrá demorar el Sistema de Detección de Llama en dar la señal de llama apagada será de tan sólo 3 segundos**.

No obstante, si consideráramos que el Sistema de Corte de Combustible pudiera tardar más de 1 segundo (como suele pasar en los sistemas con tres válvulas independientes), **el tiempo de respuesta del Sistema de Detección de Llama deberá poder ajustarse para que la acción total de la SIF no supere los 4 segundos**.

4.2 Características Funcionales del Sistema de Corte de Combustible

Como ya dijimos anteriormente, el Sistema de Corte de Combustible podrá realizarse con válvulas de shutoff independientes o por medio de un sistema integral del tipo "Trifecta".

Como **ventajas de los Sistemas tipo Trifecta** hemos visto la mayor simplicidad de cableado y la consiguiente **menor cantidad de entradas/salidas requeridas en el Logic Solver,** el **rápido accionamiento** del que estos sistemas son capaces y su **funcionamiento FailSafe**.

Como ventaja adicional podemos mencionar la menor cantidad de bridas necesarias, lo cual reducirá el riesgo de fugas de combustible en la zona, contribuyendo así a reducir el nivel de riesgo general.

Adermás, como este tipo de Sistema de Bloqueo y Venteo **ha sido homologado por FM** de acuerdo con su Norma FM 7400, **se recomienda ampliamente la utilización de los Sistemas tipo Trifecta como garantía de confiabilidad para integrar BMSIS de Nivel SIL3**.

4.3 Características Funcionales del Logic Solver

Es mucho lo que ya hemos hablado acerca de Logic Solvers para Sistemas BMS (ver SN-3121, SN-5031).

Baste con recordar que **el Logic Solver para un BMSIS deberá ser del tipo FAILSAFE De-Energize-To-Trip, deberá estar homologado para ejecutar SIFs de Nivel SIL 3 según la Norma IEC 61508, así como SIFs de protección según las Normas NFPA 85 y 86, y deberá proveer monitoreo de línea apto para Categoría 4 según ISO 13849**.

En los casos en los que se requiera, además, de Alta Disponibilidad Operativa con un muy bajo nivel de probabilidad de fallas espurias, **el Logic Solver deberá ser FAILSAFE / FAULT TOLERANT, con arquitectura integral** (CPU y Entradas/Salidas) **del tipo 1oo2D ó TMR**.

Asimismo, **se deberá garantizar que el tiempo de ciclo** ("scan" de la lógica + autodiagnóstico), **del programa de aplicación del BMSIS** (aplicativo de software del Logic Solver), **sea tal que, sumado al FFRT del Sistema de Detección de Llama, y al tiempo de respuesta del Sistema de Corte de Combustible, no lleve el tiempo total de acción de la "SIF de shutoff de combustible por apagado de llama" a un valor superior a los 4 segundos**.

5. Conclusiones

Asumamos, por todo lo expuesto, **que DEBEMOS prescribir, para toda Caldera u Horno Industrial, la utilización de un BMSIS con capacidad para ejecutar SIFs de Shutoff de Combustible por Falta de Llama de Nivel SIL 3**, compuestas, para cada Quemador por los siguientes componentes:

- **UNO o DOS Sistemas de Detección de Llama de Alta Discriminación UV+IR, cada uno con doble circuito independiente de indicación de llama apagada, con autodiagnóstico FailSafe y relé de falla independiente para cada canal, con una Tasa de Fallas Peligrosas (FRD) de 1/ 5000 años o menor y con un tiempo de respuesta por falta de llama (FFRT) ajustable hasta 3 segundos** (máximo absoluto).

- **UN Sistema de Corte de Combustible FailSafe con Doble Bloqueo y Venteo, certificado por FM según la Norma FM 7400** (con un tiempo de actuación total máximo tal, que permita un tiempo máximo de corte de combustible de 4 segundos, incluído el tiempo de ciclo del Logic Solver y el FFRT del Sistema de Detección de Llama).

Además, estas SIFs de Shutoff de Combustible por Falta de Llama serán ejecutadas por:

- **UN Logic Solver del tipo FAILSAFE De-Energize-To-Trip, homologado para ejecutar SIFs de Nivel SIL 3 según la Norma IEC 61508, así como SIFs de protección según las Normas NFPA 85 y 86, y con monitoreo de línea apto para Categoría 4 según ISO 13849.**
  En los casos en los que se requiera, además, de Alta Disponibilidad Operativa con un muy bajo nivel de probabilidad de fallas espurias, **el Logic Solver deberá ser FAILSAFE / FAULT TOLERANT, con arquitectura integral** (CPU y Entradas/Salidas) **del tipo 1oo2D ó TMR**.

Nuevamente, si no cumpliéramos con los requisitos mencionados anteriormente, **correríamos el riesgo de ser nosotros mismos los culpables de un accidente que pudiera costar muchas vidas**.

Ricardo A. Vittoni - FSS
Functional Safety Specialist

NOTA IMPORTANTE

Los esquemas eléctricos presentados en este documento son simplemente indicativos y no deberá asumirse que su implementación proveerá el Nivel SIL mencionado sin haber realizado previamente los cálculos correspondientes. El Usuario del Sistema será responsable de hacer estos cálculos así como de diseñar la arquitectura del Sistema que proveerá el Nivel de Reducción de Riesgo necesario en cada aplicación en particular.